Deutscher Bundestag **Drucksache 19/11133**

19. Wahlperiode 26.06.2019

Kleine Anfrage

der Abgeordneten Benjamin Strasser, Stephan Thomae, Manuel Höferlin, Grigorios Aggelidis, Renata Alt, Dr. Jens Brandenburg (Rhein-Neckar), Dr. Marco Buschmann, Dr. Marcus Faber, Daniel Föst, Dr. Christoph Hoffmann, Reinhard Houben, Ulla Ihnen, Olaf in der Beek, Dr. Marcel Klinge, Carina Konrad, Michael Georg Link, Oliver Luksic, Alexander Müller, Bernd Reuther, Dr. Stefan Ruppert, Frank Sitta, Dr. Marie-Agnes Strack-Zimmermann, Katja Suding, Nicole Westig und der Fraktion der FDP

Wanzen im Wohnzimmer – Überwachung durch Sprachassistenten und smarte Geräte

Weltweit steigt die Zahl digital vernetzter Geräte. Intelligente Sprachassistenten wie Alexa oder smarte Haushaltsgeräte unterstützen auch in Deutschland immer mehr Menschen in ihrem Alltag. Prognosen zufolge wird bereits in fünf Jahren jeder Privathaushalt mit rund 500 vernetzten Geräten ausgestattet sein (www.tuv.com/de/deutschland/ueber_uns/presse/meldungen/newscontentde_380800.html). Die Masse an digital vernetzten Geräten erzeugt ebenso große Mengen an verfügbaren Daten. Bisher stellte sich insbesondere die Frage nach dem Schutz dieser in privatesten Lebensbereichen entstandenen Daten vor illegalen Zugriffen.

Nach Plänen der Innenminister von Bund und Ländern sollen künftig jedoch auch die Strafverfolgungsbehörden Zugriff auf entsprechende Daten erhalten. Das Innenministerium Schleswig-Holsteins hat eine entsprechende Beschlussvorlage für die Innenministerkonferenz, die vom 12. bis 14. Juni in Kiel stattfindet, formuliert (vgl. www.zdf.de/nachrichten/heute/innenminister-vorstoss-ermittler-sollen-zugriff-auf-daten-aus-smarten-geraeten-erhalten-100.html). Ein Sprecher des Bundesministerium des Innern, für Bau und Heimat bestätigte, dass es für eine effektive Kriminalitätsbekämpfung sehr wichtig sei, dass den Sicherheitsbehörden von Bund und Ländern auch auf diesen Geräten gespeicherte Daten nicht verschlossen blieben (vgl. www.spiegel.de/netzwelt/netzpolitik/justizministerium-warnt-ermittler-vor-zugriff-auf-sprachassistenten-wie-alexa-und-siri-a-1271089.html). Das Bundesministerium der Justiz und für Verbraucherschutz verwies hingegen darauf, dass der Schutz der persönlichsten Lebensbereiche und die Freiheit jedes Beschuldigten, sich nicht selbst zu belasten, Grenzen setze, die nicht umgangen werden dürften (vgl. www.heise.de/newsticker/meldung/Justizministerium-warnt-vor-Zugriff-auf-Daten-von-Alexa-Co-4441123.html).

Aus Sicht der Fragesteller steht dieser potentielle Zugriff auf Millionen entsprechender Geräte allein in Deutschland einen inakzeptablen Eingriff in die Bürgerrechte von Millionen unschuldiger Bürger dar. Nicht nur würden die Ermittlungsbehörden im Falle des Zugriffs einen tiefreichenden Einblick in den privaten Kernbereich der Bürger erhalten. Auch bereits die Angst, dass der Staat unbemerkt mithören könnte, schränkt die individuelle Freiheit erheblich ein. So hatte schon das Bundesverfassungsgericht (BVerfG) in seinem Urteil bezüglich der

Verfassungsmäßigkeit der Vorratsdatenspeicherung betont, dass durch die vom Bürger unbemerkte Verwendung von Daten „ein Gefühl des ständigen Überwachtwerdens“ hervorgerufen werden könne (vgl. BVerfG, Urteil des Ersten Senats vom 2. März 2010 – 1 BvR 256/08 – Rn. 1 – 345). Überdies ist fraglich, welcher Wert den Daten als Beweismittel in einem Gerichtsverfahren überhaupt zugesprochen werden kann, angesichts der Gefahr der Manipulation durch illegale Zugriffe.

Wir fragen die Bundesregierung:

1. Wie erklärt die Bundesregierung den in der Vorbemerkung der Fragesteller genannten öffentlichen Dissens zwischen dem Bundesministerium des Innern, für Bau und Heimat und dem Bundesministerium der Justiz und für Verbraucherschutz zur Überwachung von Technologien wie smarten Geräten, Sprachassistenten etc.?
2. Hat die Bundesregierung inzwischen eine konsentierte Position zu der Thematik, und wenn ja, welche?
3. Unter welchen Voraussetzungen und aufgrund welcher bereits bestehenden rechtlichen Grundlage ist ein Zugriff auf die Daten von vernetzten Geräten durch die Strafverfolgungsbehörden zulässig?
4. Inwieweit und insbesondere in welcher Konstellation ist aus Sicht der Bundesregierung der Zugriff auf vernetzte Geräte auf Grundlage der Regelungen zur Beschlagnahme gemäß §§ 94 ff. der Strafprozessordnung (StPO) möglich?
5. Inwieweit und insbesondere in welcher Konstellation ist aus Sicht der Bundesregierung der Zugriff auf vernetzte Geräte auf Grundlage der Regelungen zur Quellen-Telekommunikationsüberwachung gemäß § 100a StPO möglich?
6. Inwieweit und insbesondere in welcher Konstellation ist aus Sicht der Bundesregierung der Zugriff auf vernetzte Geräte auf Grundlage der Regelungen zur Onlinedurchsuchung gemäß § 100b StPO möglich?
7. Inwieweit und insbesondere in welcher Konstellation ist aus Sicht der Bundesregierung der Zugriff auf vernetzte Geräte auf Grundlage der Regelungen zur akustischen Wohnraumüberwachung gemäß § 100c StPO möglich?
8. Inwieweit und insbesondere in welcher Konstellation ist aus Sicht der Bundesregierung der Zugriff auf vernetzte Geräte auf Grundlage der Regelungen zur Durchsicht elektronischer Aufzeichnungen gemäß § 110 StPO möglich?
9. Wie kann aus Sicht der Bundesregierung sichergestellt werden, dass der Schutz des Kernbereichs privater Lebensgestaltung im Rahmen der genannten Eingriffe gewährleisten wird, insbesondere angesichts des Umstandes, dass sich die vernetzten Geräte oftmals nicht vollständig von den Behörden steuern lassen (bitte nach einzelnen Eingriffsgrundlagen aufschlüsseln)?
10. Inwiefern müssten bestehende Regelungen ergänzt oder neue rechtliche Grundlagen geschaffen werden, um einen Zugriff auf die Daten von vernetzten Geräten durch die Strafverfolgungsbehörden zu ermöglichen?
11. Inwieweit ist aus Sicht der Bundesregierung der Zugriff auf vernetzte Geräte mit der Quellen-Telekommunikationsüberwachung gemäß § 100a StPO und dem Einsatz der Onlinedurchsuchung gemäß § 100b StPO vergleichbar?
12. Liegen nach Kenntnis der Bundesregierung bereits gerichtliche Entscheidungen vor, die sich mit der Zulässigkeit des Zugriffs auf die Daten von vernetzten Geräten durch die Strafverfolgungsbehörden auseinandergesetzt haben?

13. Unter welchen Voraussetzungen, aufgrund welcher bereits bestehender rechtlicher Grundlagen und in welchem Umfang ist Deutschland nach Ansicht der Bundesregierung verpflichtet im Rahmen internationaler Amtshilfe durch vernetzte Geräte aufgezeichnete und gespeicherte Daten an andere Staaten herauszugeben?

    Wie viele Anfragen sind der Bundesregierung in diesem Bereich bekannt?

    Wie wurde mit den jeweiligen Anfragen nach Kenntnis der Bundesregierung verfahren?

14. Inwiefern und in welchem Umfang unterfallen (lokal oder in der Cloud) gespeicherte Aufzeichnungen und Transkribierungen dieser Aufzeichnungen vernetzter Geräte nach Ansicht der Bundesregierung dem US-amerikanischen CLOUD Act?

15. Wie ist aus Sicht der Bundesregierung der Zugriff von Strafverfolgungsbehörden auf die Daten vernetzter Geräte mit dem Grundrecht auf informationelle Selbstbestimmung gemäß Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 des Grundgesetzes (GG) vereinbar?

16. Wie ist aus Sicht der Bundesregierung der Zugriff von Strafverfolgungsbehörden auf die Daten vernetzter Geräte mit dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 GG vereinbar?

17. Wie ist aus Sicht der Bundesregierung der Zugriff von Strafverfolgungsbehörden auf die Daten vernetzter Geräte mit dem Grundrecht des Fernmeldegeheimnisses aus Artikel 10 Absatz 1 GG vereinbar?

18. Wie ist aus Sicht der Bundesregierung der Zugriff von Strafverfolgungsbehörden auf die Daten vernetzter Geräte mit dem Grundrecht auf Unverletzlichkeit der Wohnung gemäß Artikel 13 Absatz 1 GG vereinbar?

19. Wie ist aus Sicht der Bundesregierung der Zugriff von Strafverfolgungsbehörden auf die Daten vernetzter Geräte mit dem Recht, dass sich ein Beschuldigter nicht selbst belasten muss, vereinbar?

20. Inwieweit nimmt nach Ansicht der Bundesregierung die Tiefe des Eingriffs durch den Umstand zu, dass es sich um einen Zugriff auf Alltagsgeräte und die von ihnen erfassten Informationen, die oftmals den privaten Lebensbereich der Bürgerinnen und der Bürger betreffen, handelt?

21. Inwieweit ist die Bundesregierung der Ansicht, dass durch Zunahme der Möglichkeiten der Überwachung die Bürgerinnen und Bürger ein „diffus bedrohliches Gefühl des Beobachtetseins“ entwickeln könnten (vgl. BVerfG, Urteil des Ersten Senats vom 2. März 2010 – 1 BvR 256/08 – Rn. 1 – 345)?

22. Wie bewertet die Bundesregierung die Aussage des Bundesdatenschutzbeauftragten Ulrich Kelber, dass es sich bei dem Vorstoß um eine verfassungsrechtlich bedenkliche Kompetenzerweiterung handle (vgl. www.zdf.de/nachrichten/heute/innenminister-vorstoss-ermittler-sollen-zugriff-auf-daten-aus-smarten-geraeten-erhalten-100.html)?

23. Wie ist aus Sicht der Bundesregierung der Umstand verfassungsrechtlich zu bewerten, dass in einem Datensatz eines vernetzten Gerätes grundsätzlich auch eine Vielzahl von Daten unbeteiligter Dritter gespeichert sind, auf die die Strafverfolgungsbehörden ebenfalls zugreifen könnten?

24. Wie bewertet die Bundesregierung die Aussagekraft von Daten von vernetzten Geräten angesichts der Manipulierbarkeit dieser Daten etwa durch Hackerangriffe?

25. Welche Schlussfolgerungen zieht die Bundesregierung aus der Manipulierbarkeit der Daten von vernetzten Geräten für ihren Beweiswert vor Gericht?
26. Für die Aufklärung welcher Straftatbestände kommt aus Sicht der Bundesregierung eine Ermächtigung der Strafverfolgungsbehörden, auf die Daten vernetzter Geräte zuzugreifen, in Betracht?

Berlin, den 19. Juni 2019

Christian Lindner und Fraktion

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333